9 INFORMATION SECURITY

The current NAS is a collection of systems, each evolving independently over time to support a major NAS functional area. As modernization proceeds, these independent systems will migrate toward an open architecture with more interaction between systems both inside and outside the NAS. While numerous benefits can be gained from open systems and standard data formats, the risk of unwanted disruptions of critical NAS services also increases. To decrease this risk, the architecture identifies key risk areas and proposes mitigating strategies.

Information security (INFOSEC) is integral to the NAS architecture. While not an obvious contributor to NAS functionality, INFOSEC is essential to ensuring the availability, integrity, and confidentiality of NAS operations. To protect NAS systems, INFOSEC must be engineered so that NAS functional performance and cost tradeoffs include appropriate protection whenever sensitive systems are involved. This includes, for example, all processing, storage, and communication of air traffic control (ATC) information. This section provides a high-level INFOSEC approach, but does not discuss detailed protective measures.

9.1 Need for Information Security

Safeguarding information systems used for NAS operations is an essential part of the NAS architecture. In addition to data directly related to ATC operations, sensitive or proprietary information pertaining to NAS users must be protected.

An effective NAS INFOSEC architecture encompasses many activities, ranging from policy to testing. These activities must be covered over the life cycle of NAS systems. The INFOSEC aspects of the architecture must define investment strategies that balance threat and potential vulnerabilities against investment costs.

9.2 Evolution of Information Security

The NAS is evolving to embrace new systems and open systems. This evolution has resulted in an increased use of common industrial standards and commercial off-the-shelf (COTS) products and a decreased use of proprietary systems. These changes emphasize the need to manage security interfaces among systems and to fully utilize the security features of COTS products to protect the NAS.

9.3 Scope of NAS Information Security

An information security architecture ensures the use of appropriate and uniform security measures across NAS subsystems, elements, and services. The architecture addresses NAS operational systems, as well as any administrative systems connected to operational systems. Interfaces between these and other systems (e.g., user systems or other government systems) are also addressed. Public networks, which are used to transfer information between facilities and systems within the NAS, are considered vital avenues of access into the NAS. The FAA will focus on ensuring information security at the interface points between the NAS and public networks.

Since the NAS is a “system of systems,” security between different systems—as well as security within individual systems—must be emphasized. Processing, storing, and transferring information within and across systems must be secure. This prevents attacks that use one weak system as an entry point from which to probe and penetrate other NAS systems. As shown in Figure 9-1, the goal of INFOSEC is to protect the availability, integrity, confidentiality, and authenticity of data used in NAS operations.

9.4 Information Security Approach

Analyses of NAS systems, along with assessments of security products and services, are used to develop security profiles. System acquisition personnel use these profiles to match characteristics of particular systems with appropriate security products and services. Coupled with appropriate policies and procedures, profiles provide an integrated approach to information security in the NAS.

A management structure will administer security processes from an operational viewpoint and participate during the acquisition phase of the life cycle. A systemwide concept of operations (CONOPS) for information security ensures uniform security measures within individual systems and compatibility across systems.

PART II

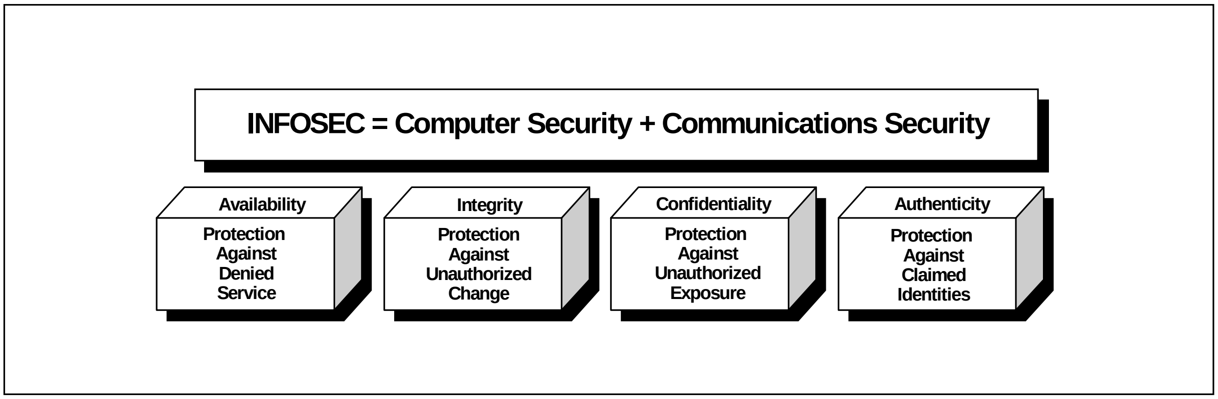

Figure 9-1. Goal of Information Security

9.5 Information Security Elements

INFOSEC policy, CONOPS, and security engineering process drive the security approach. Figure 9-2 illustrates the relationships among these elements. As a component of the NAS architecture, the security architecture provides high-level technical guidance on security-relevant structural aspects of NAS systems.

INFOSEC policy establishes basic ground rules to guide the CONOPS and Security Engineering Process, and thus guide the security approach.

The INFOSEC CONOPS is aligned with future directions for air traffic control operations, as well as with the technical and organizational changes associated with a centralized approach to NAS infrastructure management. The INFOSEC CONOPS defines functions to support the following objectives:

- Enforce INFOSEC policy
- Maintain preparedness for prompt response to rapidly changing risks and security technologies.

The INFOSEC engineering process defines acquisition-relevant INFOSEC functions that are consistent with:

- Progressive realization of NAS security protection through sound security practices

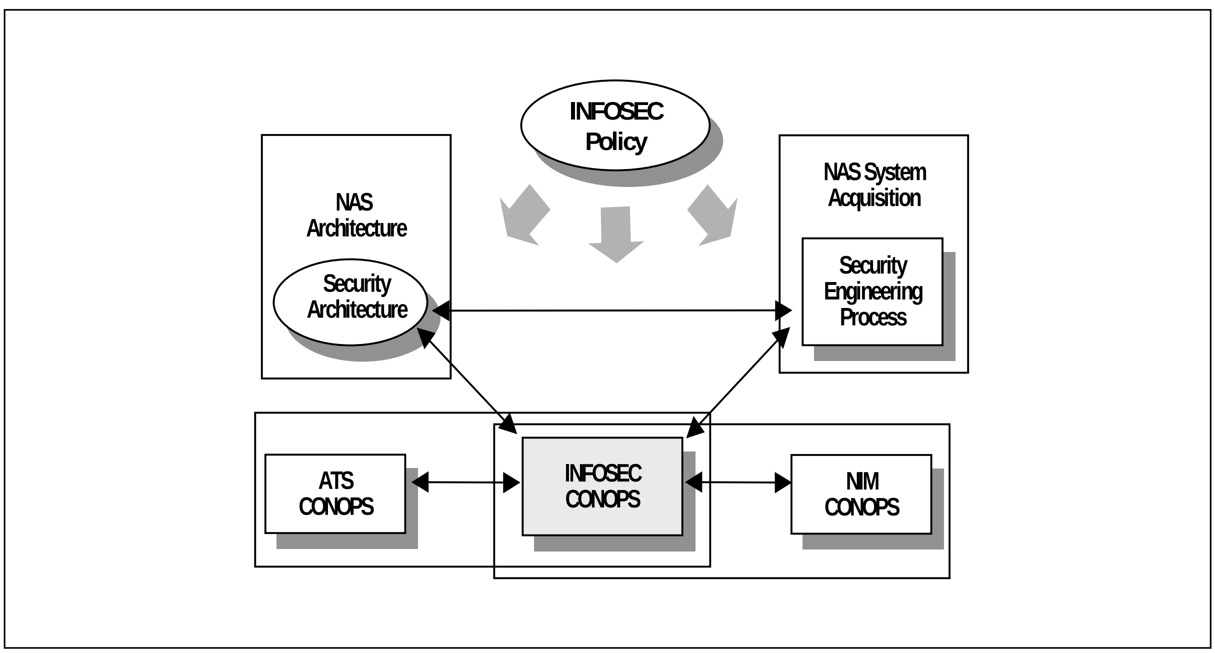

Figure 9-2. Relationships Between Major INFOSEC Elements

- Revised FAA acquisition procedures
- Fielding systems for operational use without introducing new vulnerabilities.

9.6 Technical Capabilities

As a part of the NAS architecture, INFOSEC capabilities will support multiple logical barriers to provide a layered defense of NAS systems. One barrier consists of countermeasures integrated into individual systems to protect local operation.

Another barrier is created by adding countermeasures at the entry points where external systems connect to the NAS. Countermeasures include firewalls, proxy servers, and security gateways to control communications access in a distributed network. This barrier secures NAS operations against unauthorized access from external systems. A further barrier consists of countermeasures to authenticate users within communities-of-interest, such as air traffic control, air traffic management, and flight services. Common security services support the various barriers. For example, one service involves audit collection and system monitoring, and another service provides tools for security administration.

9.7 NAS Functional Areas

9.7.1 Communications

Air-air, air-ground, and ground-ground communications have specific characteristics that must be evaluated separately to determine their contribution to vulnerability and risk to the systems within the domains over their life cycles. The FAA information security engineering process will be applied in determining communications vulnerabilities and the required countermeasures needed to control communications-related risks. Future security services will preserve the availability, integrity, confidentiality, and authenticity of NAS communications.

9.7.2 Navigation, Landing, and Lighting Systems

With precision landing services eventually depending primarily on the use of Global Positioning System (GPS) signals augmented by Wide Area Augmentation System (WAAS) and Local Area Augmentation System (LAAS) differential correction signals, there is a need to protect these systems from harmful interference. The FAA is currently working to develop safety and system security countermeasures for satellite-based navigation and landing systems to prevent or mitigate interference. The backup navigation and landing system capabilities that are needed to protect against intentional jamming and signal interference will be defined.

The FAA and the users, through RTCA, Inc., are currently reviewing the backup requirements for GPS. The likelihood of interference is the primary threat to GPS navigation. Any backup determined as being necessary must support at least nonprecision approach capabilities, for it is in the landing phase that interference will be most disruptive.

9.7.3 Surveillance

The evolution of the surveillance system architecture introduces new information security risks for automatic dependent surveillance broadcast (ADS-B) surveillance reports. Potential surveillance security concerns include interference with WAAS correction signals, which affects the accuracy of ADS-B data; interference with GPS signals, which denies ADS-B service in the affected area; and message flooding of the surveillance system.

Security features are needed for the surveillance systems to ensure continued operations during these types of events, which is one of the reasons for continuing secondary surveillance radar (SSR). Provisions will also be considered for detecting unusually high message activity on surveillance inputs and generating a warning. Sharing surveillance information will necessitate special security provisions, including access control, user verification functions, and restrictions on the types of information that each user group can access.

9.7.4 Avionics

Avionics is the primary airborne component of the communications, navigation, and surveillance systems. The security considerations that apply to the avionics interface with these systems are summarized below. Using the NAS information security engineering process, the integrated product team (IPT) will work with the NAS Information Security Program during the entire life cycle of a fielded system, especially during functional upgrades and technology refresh, to identify the need for protection mechanisms.

- *Communications.* The next-generation air-ground communications system (NEXCOM) radio will be used to exchange real-time, safety-critical flight clearance information with the cockpit. The NAS information security engineering process will identify security provisions and countermeasures to be incorporated in the NEXCOM system design.
- *Navigation.* GPS, WAAS, and LAAS will be used as the primary means (systems) of navigation. Intentional and unintentional interference with GPS signals may result in a hazard that affects many aircraft simultaneously. This potential problem will be fully evaluated within the overall GPS, WAAS, and LAAS operational evaluation programs.
- *Surveillance.* The NAS architecture includes an automatic dependent surveillance (ADS) position reporting capability. Security provisions will be developed against possible interference and erroneous data transmission.

9.7.5 NAS Information Services for Collaboration and Information Sharing

Security will become a more complicated issue as the NAS-wide information network evolves. The sources and users of electronic data will increase substantially, as will the quantity and types of data available. Protecting the integrity and privacy of information will be critical to NAS-wide information network effectiveness (i.e., users must have confidence in data they access and that proprietary data are protected). New security systems and procedures will be implemented. Authorized users will have access to information—whenever and however they require—and unauthorized individuals will be denied access.

9.7.6 Traffic Flow Management

The traffic flow management (TFM) system allows users to obtain NAS information, electronically transfer flight plan data, and develop flight plans collaboratively. The TFM system receives, stores, and disseminates sensitive data from airline operations centers (AOCs), which will require solid information security measures. These security measures include logical separation of administrative and operational data, protection of sensitive AOC scheduling data, Internet access controls, firewalls, role-based access controls, and security gateways between the TFM network and any connected, nonsecured systems.

9.7.7 En Route

En route automation will be extended to support collaborative processing, flexible airspace structures, dynamic routes, and self-separation. En route technology will transition from relatively closed systems to open systems. Communications among systems will increase significantly, and data messages will replace many existing air-ground voice communications. New types of data structures will be implemented, and new classes of users will need to work with en route data.

Throughout en route modernization, service providers and users will need to identify appropriate security services. These services include authentication to protect the system from unauthorized access, integrity to protect messages containing sensitive information from corruption, and encryption to protect the privacy of data or to enhance authentication. Additionally, security training and administration will be the primary protection mechanisms during the operations and maintenance phase of the life cycle.

9.7.8 Oceanic and Offshore

Two classes of security are relevant to the oceanic system. The first is protection of the air-ground and ground-ground communications links. The second is protection of the ground-based components of the oceanic systems, which include automation and communications subsystems. The key services are user identification and authentication, access control, and an interface protection mechanism.

9.7.9 Terminal

The terminal domain contains several sensitive decision support systems that require security services. These services include authentication to protect the system from unauthorized access, integrity to protect messages containing sensitive information from corruption, and encryption to protect the privacy of data or to enhance authentication. In addition, security training and administration are key protection mechanisms during the operation and maintenance phase.

9.7.10 Tower and Airport Surface

The tower/surface automation and communications subsystems include a surface movement adviser (SMA) system and an air-ground tower data link service (TDLS). These systems must be protected against security breaches. For example, the SMA system will interface with AOC facilities at airports. Hence, there is a need to protect schedule and aircraft movement data on the SMA communications circuits and in the FAA and airline data bases.

Security concerns include unauthorized user access and modification or destruction of sensitive information used for surface operations control. Another concern is the air-ground data link, which will handle safety-critical clearance and real-time messages. Potential security breaches include unauthorized clearance transmissions and modification of messages on ground links. Provisions to mitigate security risks may include installation of security gateways between the FAA operational system and outside users and between the NAS information system and the TDLS access controls; message origin and message traffic verification; and security protection of surface control and movement data bases.

9.7.11 Flight Services

Flight services interacts with pilots and agencies outside the FAA. To meet its objectives, flight services must also interface with other NAS systems, including the weather and radar processor (WARP), the weather message switching center replacement (WMSCR), the en route automation system, and traffic flow management systems. Thus, the flight service system (i.e., the Operational and Supportability Implementation System (OASIS)) needs security services that include access control, user identification, and security gateways to protect availability, integrity, and confidentiality for itself and other interconnected systems.

9.7.12 Aviation Weather

Weather products are received both from FAA sensors, the National Weather Service (NWS), and commercial vendors. Weather messages flow among the FAA sensors, the integrated terminal weather system (ITWS), WARP, operational ATC systems, and the user community. Weather systems require protection against injection of false weather messages, unauthorized access, and unauthorized modifications of weather data bases. Security provisions for the weather subsystem will include access control, message sender authentication, and audit functions to record all messages and to identify the source of each message.

9.7.13 Infrastructure Management

NAS Infrastructure Management (NIM) tools interface with all other NAS systems, and its security access must be protected. For this reason, the management and control of NAS security services is a logical candidate for future inclusion in the NIM architecture. NIM tools could be used to collect NAS-wide subsystem security data for reporting and auditing purposes and to perform NAS-wide intrusion detection.

Within NIM tools, INFOSEC requirements are based on the NIM protection profile and vulnerability assessment. Meeting requirements for service availability, access control, authentication, nonrepudiation, and confidentiality will ensure adequate security for NIM tools. In particular, appropriate security gateway services are available to provide proper access control between NIM tools and other NAS systems.

Security management will allow the FAA to protect NIM tool data via user identification, authentication, and access control mechanisms. NIM tools could also support NAS-wide security management, such as detecting and logging NAS infrastructure security violations for reporting to FAA management.

9.8 NAS Information Security Cost

The FAA's estimated costs for NAS information security modernization are depicted in Figure 9-3. These costs include initial estimates for developing INFOSEC requirements and limited IPT support. The NAS INFOSEC process is awaiting investment analysis and Joint Resources Council (JRC) determination.

PART II

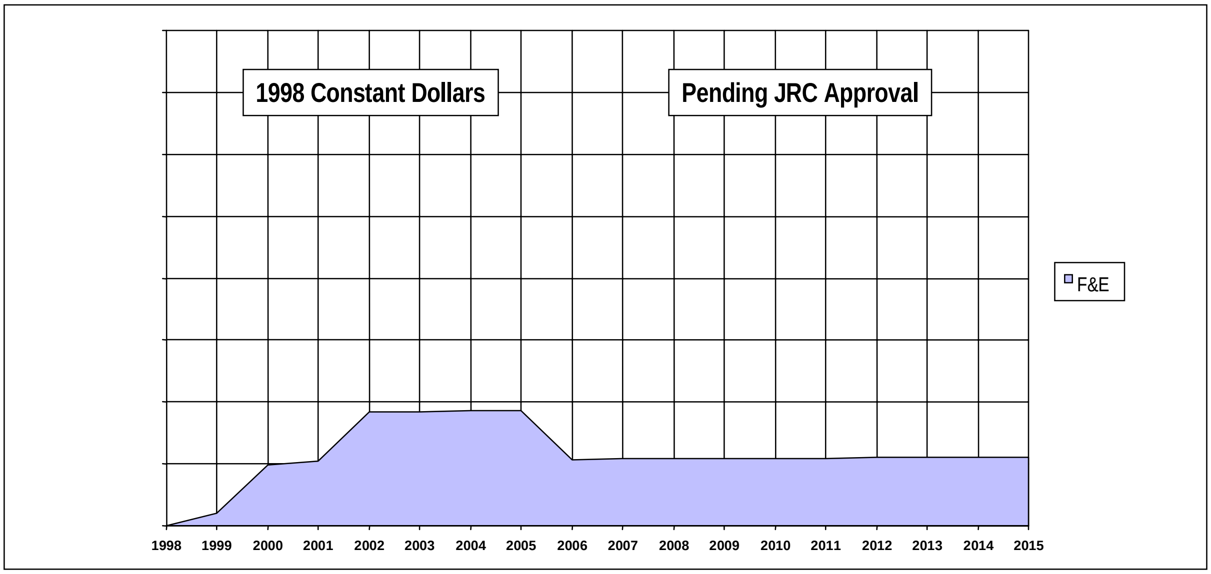

Figure 9-3. Estimated INFOSEC Costs

9.9 Summary

The present NAS is robust and extraordinarily resilient. NAS modernization includes the addition or revitalization of many programs. On the one hand, these programs bring new capabilities that enable future benefits. On the other hand, expanded functionality, greater connectivity, and well-understood commercial technology call for increased INFOSEC vigilance. The future NAS must implement a coherent INFOSEC architecture that mitigates these risks. Protection must extend throughout a system's life cycle. By applying sound INFOSEC principles during planning and design, the future NAS will retain its present resilience while addressing future concerns at acceptable costs.

The *National Airspace Architecture Version 4.0* does not provide specific architecture details for INFOSEC. This information is considered sensitive and would increase NAS vulnerability. The information security architecture is provided on a need-to-know basis.

The next section describes the role that research, engineering, and development plays in the modernization process. Successful research efforts are the key to unlocking the potential of new and, in some cases, yet to be discovered technologies.